I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

MATTHEW HOTTELL*

Defaults vs. Rational Choice: The Case of Home-Based Wireless Security

Abstract: Wireless routers are appearing in homes in increasing numbers. Many of these routers are left in a default configuration completely without security, and even more are not effectively secured. At the same time people are increasingly reporting concerns about privacy and security online.[1] What factors contribute to the general state of insecurity in home-based wireless networks? Building on past work on the economics of security and privacy, this paper develops three rational choice economic hypotheses that predict the adoption of security measures for wireless routers. According to previous work, the risks associated with a lack of security (i.e., increased housing density or a greater number of assets to protect) should predict the adoption of security technology. Other researchers have argued that privacy and security are simply not generally understood by consumers. Thus, higher levels of formal education among consumers might predict adoption. This paper fully develops these hypotheses and tests them empirically.

A series of wardrives were conducted to examine the relative state of security of wireless access points in neighborhoods representing key demographics.[2] After a comprehensive study of the resulting 2500 data points, I discovered that the only

---

* The author would like to thank Jean Camp of the Indiana University School of Informatics for her advice and mentorship during this project. Informatics students Matt Deniszcuk and Andrew Carter were instrumental in wardriving.

[1] Jonah D. Seiger, "Privacy, Security & Trust on the Political Web: Factors that Influence the Willingness of Internet Users to Provide Sensitive Personal Information to Political Web Sites," (The Institute for Politics, Democracy & the Internet, March 2003), http://www.ipdi.org/uploadedfiles/privacy_security_and_trust_survey_final.pdf (accessed October 31, 2007).

[2] "Wardriving" is the act of searching for and cataloging wireless networks by a person in a moving vehicle using a wireless-equipped computer, such as a laptop or a PDA.

indicator of implementation of wireless security measures appears to be router type. Routers with default security configuration were found to be secure 97% of the time, while identifiable Linksys Secure Easy Setup routers were only secure 88% of the time. The percentage of routers classified as securely configured in the entire study was 61%.

The surprising results of this extensive wardriving effort are that interface design and default settings appear to be the dominant factors in determining utilization of security measures, indicating consumers are making rational choice decisions in the area of home wireless security. The rational economics hypotheses I tested do not predict adoption of security measures in the case of home-based wireless. Finally, strictly market-based policies would arguably be inadequate. In closing, alternate bases for policy development are examined and future work to test defaults and usability as policy tools is described.

I. INTRODUCTION

This paper reports on the factors that have been argued in empirical studies and quantitative models of security decision-making to predict adoption of security and privacy mechanisms. This paper describes and evaluates the factors that bear on the implementation of encryption in wireless access points. Section I describes consumer privacy and security concerns at a general level. Section II provides more detail on the specific motivation for the experiment conducted; Section III describes the wardriving experiment. The results of the study are reviewed in Section IV; the implications of the findings are discussed in Section V. Section VI provides a summary of my findings, a discussion of the policy implications of the findings and the direction of further research on the subject, as well as concluding remarks.

A. THEORY AND MOTIVATION

This section begins with a basic discussion of privacy and security theory followed by a description of the specific work on the economics of security that motivated the hypotheses underlying my study.

The advent of the Information Age has created a new set of economic factors that have hastened the erosion of personal privacy. Computing systems have increasingly become interconnected, while computing devices have been integrated into practically all aspects of our lives. This tendency toward connection and integration creates an environment where private personal information can be collected and traded; intrusive spam email can reach us in our homes and websites can track our every surfing move online.

But what exactly is privacy? Jim Harper of the Cato Institute defines privacy as "the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values."[3] Under this definition, acceptable privacy levels depend on the judgments of individuals, not society as a whole. Furthermore, this view does not treat privacy as a right *per se*, but as a personal condition that must be maintained by "exercising personal initiative and responsibility."[4] In other words, each individual is responsible for personal vigilance when protecting her personal level of privacy in the face of privacy-eroding efforts.

For the purposes of this experiment, we define privacy to consist of three elements: secrecy, autonomy, and seclusion. Secrecy refers to the right to control the proliferation of personal information, autonomy is the right to be free from observation, and seclusion is the "right to be let alone."[5] Each of these aspects of privacy is threatened by participating in online activities. For example, secrecy can be negatively impacted when a website shares the personal information it acquires from clients with outside parties. Seclusion can be violated by spam, spim, or pop-up advertisements.[6] Autonomy is impacted when advertising companies use cookies to track people as they view pages across multiple sites as well as by the use of identifying technologies.

"Security" can be defined as the state of being free from risk or exposure to damage from accident or attack.[7] Security consists of the

---

[3] Jim Harper, "Understanding Privacy – and the Real Threats to It," *Cato Institute: Policy Analysis*, no. 520 (August 2004): 2, http://www.cato.org/pubs/pas/pa520.pdf (accessed October 31, 2007).

[4] Ibid., 5. These terms, used to describe a "right to privacy," were coined by Justice Brandeis in his dissent to the majority opinion in a vary famous Fourth Amendment United States Supreme Court case, *Olmstead v. United States*, 277 U.S. 438, 478 (1928).

[5] L. Jean Camp and Carlos A. Osorio, "Privacy-Enhancing Technologies for Internet Commerce," (working paper, John F. Kennedy School of Government, Harvard University, August 2002), http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP02-033/$File/rwp02_033_camp.pdf (accessed October 31, 2007); see also *Olmstead v. United States*, 277 U.S. 438, 478 (1928).

[6] "Spim" is a term referring to unsolicited messages received via instant messaging applications.

[7] Seymour Bosworth and M.E. Kabay, eds., *Computer Security Handbook*, 4th ed. (New York: John Wiley & Sons, 2002), 1–2.

set of means by which consumers limit risks to the resources they own. These protected resources can be electronic files or physical property, as well as resources like network capacity, human attention span, behavior within the home, reputation, and information about surfing habits.

Security has three goals: confidentiality, integrity, and availability.[8] First, confidentiality is the security goal of preventing unauthorized access to resources.[9] Physical security measures that fall into this category include the use of window blinds, fences, and post office boxes. Policy measures include the creation and utilization of a do-not-call list. The do-not-call list provides security by preventing outside intrusion into the sanctity of the home and abuse of the call-recipient's resources, including the use of the recipient's telephone line and her attention. Other technology-based confidentiality controls include measures such as firewalls and encryption. Authentication and authorization systems are double-edged swords that can be used to protect confidentiality by limiting access to data or to violate confidentiality by implementing surveillance.

Second, integrity is the attempt to maintain resources free of unauthorized alteration; third, availability is the goal of ensuring that resources remain accessible when required by authorized entities.[10] Many security controls work to meet multiple security goals. For example, the aforementioned do-not-call list also operates as an availability measure; it increases the availability of telephone lines by freeing them from unwanted calls.

Security controls are implemented based on the individual's perception of a threat to personal resources. Risk can be defined as the probability that a particular attack will occur multiplied by the loss potential of the attack.[11] If either factor is perceived to be low, then it is unlikely that any security measures will be introduced.

What are the risks associated with the erosion of privacy? One potential use of personal information is price discrimination. Price discrimination is the practice of charging different prices for the same good based on the consumer's perceived willingness to pay. This allows a seller to sell goods at several points along the demand

---

[8] Ibid., Chap. 5 Sec. 1.

[9] Ibid.

[10] Ibid.

[11] Ibid.

curve.[12] In order for sellers to effectively price discriminate, accurate personal information is required. Price discrimination reduces the consumer surplus which maximizes cost efficiency for the seller/producer. The seller, therefore, has an economic incentive to gather enough personal information to set a price for a consumer that is closer to the price that the consumer is willing to pay for a good. The consumer has a competing economic interest in keeping the same information private.

Identity theft presents a combined security and privacy risk. Identity theft is the capture and use of personally identifying information for the purpose of conducting financial fraud.[13] The true cost of such an attack to the consumer is not measured in terms of the money stolen using the fraudulent credentials because liability in fraud cases is limited in many jurisdictions. Rather, the actual cost to the victim is measured in loss of credit standing and the resources spent to fix the individual's financial records, which can often take years.[14] Victims of identity theft can also face loss in the form of permanent damage to their reputation and relationships as well as job loss when credit cards issued in their name to identity thieves are used for criminal or embarrassing activities such as obtaining child pornography.[15]

A relatively new factor in the online privacy equation is the emergence of wireless networking technologies. The creation of the graceful and efficient wireless protocols defined as the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard has made

---

[12] Alessandro Acquisti and Hal R. Varian, "Conditioning Prices on Purchase History," *Marketing Science* 24, no. 3 (2005): 367; Andrew Odlyzko, "Privacy, Economics, and Price Discrimination on the Internet," in *Proceedings of the 5th International Conference on Electronic Commerce 2003, ACM International Conference Proceeding Series* 50 (Boston, Massachusetts: ACM Press & Addison-Wesley Professional, 2003): 356, http://portal.acm.org/citation.cfm?id=948051 (accessed October 31, 2007); Luc Wathieu, "Privacy, Exposure, and Price Discrimination," (working paper, Marketing Unit, Harvard School of Business, Harvard University, 2002).

[13] Dorothy E. Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999): 241–46.

[14] Ibid.; Synovate, *Federal Trade Commission - Identity Theft Survey Report* (McLean, VA: Synovate, 2003), http://www.consumer.gov/idtheft/pdf/synovate_report.pdf (accessed October 31, 2007).

[15] CBC News, "Global Child Porn Probe Led to False Accusations," *Canadian Broadcast Corporation*, March 14, 2006, http://www.cbc.ca/world/story/2006/03/14/landslide-porn060314.html (accessed October 31, 2007).

participating in the online world via wireless access easier and more convenient. The system was initially confined to business use due to prohibitive costs, but recent years have witnessed a large increase in the home adoption of wireless devices. Wireless routers designed for home use are fairly similar in price and security capability. This technology allows easier access for everyone and as a result, wireless security can be problematic. Instead of requiring a physical connection to a home network, anyone with the proper hardware and software can connect to a wireless device and potentially access both the private internal network and any connected wide area network (WAN). The intruder need only be in fairly close proximity to the wireless device to access the network. Security mechanisms such as encryption and Media Access Control (MAC) address authentication are available via configuration in practically all home-based wireless routers.[16]

Unsecured wireless networks present cybercriminals with virtual immunity to prosecution. Anyone can drive near an open node, connect to the Internet by accessing the network bandwidth resources supplied by the router, and then engage in a variety of activities ranging from sending spam emails to downloading child pornography to distributing malicious code. Once done, the attacker can simply drive away leaving little evidence of its presence. Perhaps an even more likely scenario is a neighbor using an open access point to share and download copyrighted material. Each of these actions carries clear economic costs that can potentially be borne by the actual victim of the crime (loss of property or system damage, etc.) as well as the owner of the open access point (lawsuits or criminal investigation, etc.).[17] The recent activity of the Recording Industry Association of America (RIAA) in pursuing copyright infringement cases demonstrates this point. These lawsuits associated an Internet Protocol (IP) address with the alleged distribution of copyrighted content.[18] The RIAA was able to obtain defendants' names by subpoenaing Internet Service Provider (ISP) records.[19] An out-of-court settlement for a copyright infringement suit brought by the RIAA is usually

---

[16] Bosworth and Kabay, *Computer Security Handbook*, 1–2; Denning, *Information Warfare and Security*, 241–46.

[17] CBC News, "Global Child Porn Probe Led to False Accusations."

[18] Ray Beckerman, "How the RIAA Litigation Process Works," *Recording Industry vs. the People*, October 10, 2007, http://info.riaalawsuits.us/howriaa_printable.htm (accessed October 31, 2007).

[19] Ibid.

$3750 regardless of the number of infringement counts.[20] The RIAA will generally seek $750 in damages per song if the case goes to trial.[21] In the case of unsecure wireless routers, the defendant in these suits may have had nothing to do with the infringement activity but will bear the cost anyway.

Other risks impose costs that fall more squarely on the owner of the wireless access point. These costs can include the loss of information stored on computing devices connected to the wireless node, including financial and personal information, which could be used in an identity theft attack. If the node is left in a complete default state, an attacker can access the router administration panel, reconfigure the Domain Name System (DNS) settings to point to a different IP address, and engage in a pharming attack that can reveal account username and password information for websites that contain financial information.[22] In addition, an attacker can collect and decipher wireless packets and track the activities of computers using that wireless node.[23] Therefore, a motivated and competent attacker can potentially gather a variety of sensitive information about a victim by engaging in activities such as monitoring web surfing habits and reading emails.

One potential solution is to encrypt the network traffic. Implementing encryption technology on a wireless router helps to meet several security goals. Encryption protects confidentiality by preventing access to content during transmission: files, emails, and URLs. An attacker may still be able to intercept the encrypted transmission but will not be able to decrypt the content.[24] Encryption preserves integrity by preventing tampering with files, transmissions, and configurations. Encryption secures availability by blocking attackers' use of bandwidth and by reserving the resource for authorized individuals. Therefore, implementing encryption on a home-based router helps protect all three aspects of personal security.

---

[20] Ibid.

[21] Ibid.

[22] Alex Tsow, "Phishing with Consumer Electronics - Malicious Home Routers," (workshop, Models of Trust for the Web: 15th International World Wide Web Conference, Edinburgh, Scotland, May 22-26, 2006): 1–16 (available at http://www.cs.indiana.edu/~atsow/papers/mal-router-long.pdf).

[23] Bosworth & Kabay, *Computer Security Handbook*, Chapter 8 Section 3.

[24] Denning, *Information Warfare and Security*, 286–310.

Home-based wireless access points are usually installed by non-technical consumers and are often left in a default, unsecure configuration. There are a variety of reasons why consumers might leave their wireless access points unsecured. One reason is that the owner may wish to share an existing Internet connection as a public good. Many coffee shops use this strategy to attract and retain customers. Another reason consumers do not secure their wireless access points is a lack of knowledge. Effectively securing a wireless router without assistance requires an understanding of several basic encryption and networking concepts which many consumers simply lack. An access point will generally work in its default, unencrypted configuration, when the correct cables are plugged into the router and it is turned on. "Plug-and-play" results in many user-installed systems that remain unprotected.

Some wireless consumers do not secure their devices because they do not understand the risks associated with an open node, while others understand the risk but judge the risk to be small enough to accept. This creates a problem in that either many consumers do not know what can be done with the information they make available, or they do not understand the complicated nature of the impact of the threat.[25] A recent study of Facebook.com showed that many consumers willingly place sensitive private information online. When the consumers were asked if they wished for the information to be public, they said they wanted it to remain private.[26] Another issue is that many users may have developed the wrong mental model of what their expected contribution to security should be, based on the metaphors they encounter.[27] For example, if the metaphor used for security is "information warfare" then the average citizen of the Internet might

---

[25] For a discussion of the issue, see Adam Shostack and Paul Syverson, "'People Won't Pay for Privacy,' Reconsidered" (2nd Annual Workshop on Economics and Information Security, College Park, MD, May 29, 2003) http://www.cpppe.umd.edu/rhsmith3/papers/Final_session3_shostack_privacy.pdf (accessed November 5, 2007) (A later version, "What Price Privacy?," is available here http://chacs.nrl.navy.mil/publications/CHACS/2004/2004shostack-valupriv.pdf (accessed October 31, 2007)); L. Jean Camp and Lewis Stephen, "Economics of Information Security," *Advances in Information Security* 12 (2004): 7–20.

[26] For a discussion of the issue, see Ralph Gross and Alessandro Acquisti, "Information Revelation and Privacy in Online Social Networks," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (New York, NY: ACM, 2005) http://portal.acm.org/toc.cfm?id=1102199 (accessed October 31, 2007) (scroll down to the "Privacy Issues in Practice" session to access the paper).

[27] L. Jean Camp, "Mental Models of Security," *IEEE Technology and Society* (forthcoming).

believe that fighting back against cyber-guerillas should be left up to the security professionals, while they simply pay their "Internet taxes" to their ISP.

Whatever the case may be, wireless consumers may believe that the cost of implementing and maintaining wireless security measurably lowers the benefits of wireless consumption.[28] For example, the implementation of an access control list security mechanism requires that any new devices connected to the router first be registered. Assuming the owner knows how to accomplish this task, the process of finding the MAC address of the new device, logging in to the wireless router and entering the new MAC address into the database must be performed each time the owner wishes to connect a new device to the network. The cost of performing this series of steps may be too high, particularly for the uninformed user.

II. PREDICTORS OF HOME-BASED WIRELESS SECURITY

This section more closely examines the factors that may impact the security configuration of wireless devices.

A. IS EDUCATION THE PROBLEM?

One factor that may predict wireless security is the education level of the consumer. As noted above, implementing wireless security requires a basic level of networking knowledge that most consumers do not have. Effective education could give consumers this basic knowledge and allow them to make better choices about protecting their privacy. Education in a formal college or university setting might create an environment where consumers are exposed to more information about technology in general and specifically wireless networks. Concurrent study results indicate that wireless security rates in predominately student populations increased 9% after the university launched a security awareness campaign.[29]

One could also argue that one of the benefits of a formal higher education is a better understanding of the risks of privacy erosion. Hal Varian, Fredrik Wallenberg and Glenn Woroch found that years of

---

[28] Kai-Lung Hui and I.P.L. Png, "The Economics of Privacy," *Handbook in Information Systems* 1 (2006), http://www.comp.nus.edu.sg/~ipng/research/privacy_HISE.pdf (accessed October 31, 2007).

[29] M. Deniszczuk, Matthew P. Hottell, and D. Carter, *Does Education Work? A Quantitative Evaluation of the Behavioral Effects of Security Education* (forthcoming).

formal education was a significant predictor of whether people had signed up for the national do-not-call list.[30] This suggests that more highly-educated people understand the inherent risks and are more likely to take steps to protect their privacy. On the other hand, Wathieu and Friedman found that individuals are already generally aware of privacy risks and need no prompting to be concerned.[31]

Hypothesis 1: Higher education level predicts greater adoption of wireless security.

If education is found to be a predictor of wireless security, the obvious response is a call for better educational initiatives to empower naive consumers as they attempt to make decisions about wireless security and privacy risks.

B. ARE PRIVACY AND SECURITY LUXURY GOODS?

By definition, a luxury good is one that is consumed disproportionately or solely by the wealthy.[32] Can security and privacy be considered luxury goods? Varian, Wallenberg and Woroch found that consumers at the highest income level (>$100,000 per household) were the most likely to sign up for the do-not-call list.[33] This may indicate either that people who are wealthier are more likely to value their privacy or that the comparatively wealthy understand the potential risk of privacy erosion.

Shostack and Syverson point out that consumers often pay for goods or services that enhance privacy and that even the most uninformed wealthy person is better able to pay to have a

---

[30] Hal Varian, Fredrik Wallenberg and Glenn Woroch, "Who Signed Up for the Do-Not-Call List?" (The Third Annual Workshop on Economics and Information Security, University of Minnesota, May 13, 2004): 2, http://www.dtc.umn.edu/weis2004/varian.pdf (accessed October 31, 2007).

[31] Luc Wathieu and Allan Friedman, "An Empirical Approach to Understanding Privacy Valuation," (The Fourth Workshop on the Economics of Information Security, John F. Kennedy School of Government, Harvard University, June 3, 2005): 6, http://infosecon.net/workshop/pdf/WathFried_WEIS05.pdf (accessed October 31, 2007).

[32] Yacine Aït-Sahalia, Jonathan A. Parker and Motohiro Yogo, "Luxury Goods and the Equity Premium," *The Journal of Finance* 59, no. 6 (December 2004): 2959–3004, http://www.princeton.edu/~yacine/richc.pdf (accessed October 31, 2007).

[33] Varian, Wallenberg and Woroch, "Who Signed Up for the Do-Not-Call List," 13.

knowledgeable person configure his or her wireless router to provide maximal security than a less well-off counterpart.[34]

One of the most likely outcomes of privacy erosion is price discrimination.[35] Price discrimination requires good information to be effective, and price discrimination affects more adversely affects those who have the means to pay more for a good.[36] Therefore, one would expect that the wealthy would have greater incentive to protect their information assets knowing that the release of that information could bear a real cost in terms of a higher price paid for goods.

By definition, a wealthy person has more assets to protect. Extortion, loss of income due to reputation damage, or seizure of property are risks associated with a secure wireless router that increase correspondingly in absolute terms with wealth.[37]

Hypothesis 2: Higher income predicts greater adoption of wireless security.

Income could be highly correlated with education; therefore, wealthier consumers may also have a better understanding of the risks and be better prepared to mitigate them. In the regression discussed below, these variables were treated separately. This is feasible due to the demographics of the neighborhoods chosen.

C. Is Population Density an Indicator of Wireless Security?

There are many reasons why population density may be a good predictor of higher levels of wireless security. One such reason is that some apartment complexes provide free Internet access to their residents. These complexes often engage in education campaigns to encourage residents to secure their access points, thereby raising awareness of security and privacy issues in the complex. Another consideration is that it may be easier to identify local experts when population density is high. These experts may help increase the general level of security in the area by sharing their knowledge with others or by actually configuring other access points.

---

[34] Shostack and Syverson, "What Price Privacy?," 9–10.

[35] Odlyzko, "Privacy, Economics, and Price Discrimination on the Internet," 358–60.

[36] Ibid.

[37] Seiger, "Privacy, Security, and Trust on the Political Web."

Yet the core reason to expect higher population density to result in better security is risk. Risk of abuse is greater in terms of the likelihood of malicious action. Detection of a malicious actor is more difficult. For someone living in a remote location, the detection of potential attackers is fairly easy as it might involve recognizing that there is a strange vehicle adjacent to the consumer's home. Identifying potential attackers in a highly populated area is not so straightforward. There could be dozens of people who have the ability to access another person's wireless device from the privacy of the attacker's home. This occurs outside public view and beyond observation by the router's owner. Assuming that the probability that a person is an attacker is evenly distributed, higher population areas are therefore subject to a greater risk of attack. The sheer number of potential attackers who can access a wireless device in a densely populated area may create an incentive for the consumer to invest more resources to implement secure wireless.

Hypothesis 3: Higher population density predicts greater adoption of wireless security.

Wealth increases the magnitude of loss or loss potential. Density increases the probability of exposure to an attack to the extent that it decreases the attacker's risk of detection.

III. EXPERIMENTAL DESIGN

Data about the state of individual wireless access points was collected in a "wardrive" of sixty-two neighborhoods in a small college town. The neighborhoods surveyed represented a wide range of economic and educational demographics, and included both apartment/condominium complexes as well as single-family homes. The data was collected using two different laptop computers, one with a GPS unit attached for accurate plotting of access points. The software utilized for the data collection was NetStumbler, available at http://www.netstumbler.org.

Initially, over 3,000 access points were identified during five separate wardriving sessions which lasted a total of twelve hours. Any commercially owned access points, identifiable either by Service Set Identifier (SSID) or wireless router maker were purged from the data set in an attempt to limit data points to home-based consumers. All unique access points appearing in more than one neighborhood were also discarded to avoid data duplication. Three neighborhoods in which less than eight access points were present were dropped from

the data set as well, giving us a final total of fifty-nine neighborhoods surveyed and 2,443 individual access points recorded.

Once access point data was collected, each neighborhood was given a score reflecting the percentage of wireless access points that were identified as secure in that area. For purposes of this study, a secure wireless access point is defined as one that utilizes any form of encryption technology. A variable named *edlevel,* representing the percentage of residents with at least a bachelor's degree as determined by US Census Track (2000 Census) data, was added to each neighborhood to test Hypothesis 1. For Hypothesis 2, a variable named *income,* representing consumer income level, was approximated using rental rates for apartments and a calculated mean mortgage payment (10% of home value down, amortization over 30 years at 7% interest) for homes. Finally, a dummy variable named *pdensity,* representing high or low population density, was assigned to each neighborhood to test Hypothesis 3. A regression was then run using the following equation:

$$\%\ secured\ wireless\ points = \beta_0 + \beta_1 * edlevel + \beta_2 * income + \beta_3 * pdensity$$

IV. RESULTS

The results of the regression can be seen in Tables 1 and 2 below. None of the variables were found to be significant; therefore, we must reject all three hypotheses and conclude that income, education level, and population density are all not predictors of increased wireless security.

Table 1: Regression statistics

Regression Statistics	
Multiple R	0.1181
R Square	0.0140
Adjusted R Square	-0.0398
Standard Error	0.1342
Observations	59

Table 2: Parameter estimates

	Coefficients	*Standard Error*	*t Stat*	*P-value*
Intercept	0.665802	0.067813	9.818	0.00000
Edlevel	-0.000815	0.000998	-0.817	0.41736
Income	-0.000008	0.000047	-0.162	0.87170
Pdensity	-0.002968	0.038681	-0.077	0.93911

Chart 1: % Wireless Secured vs. Education Level

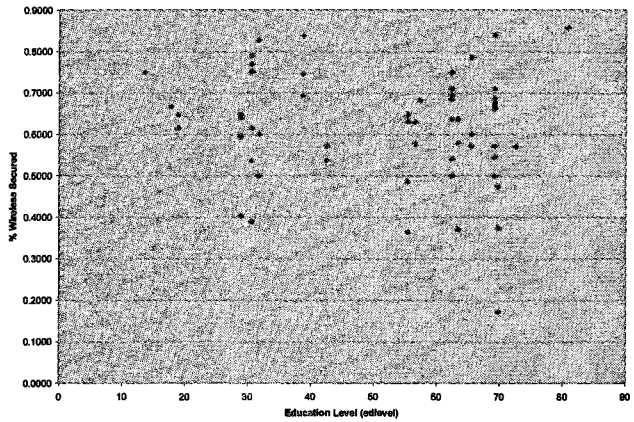
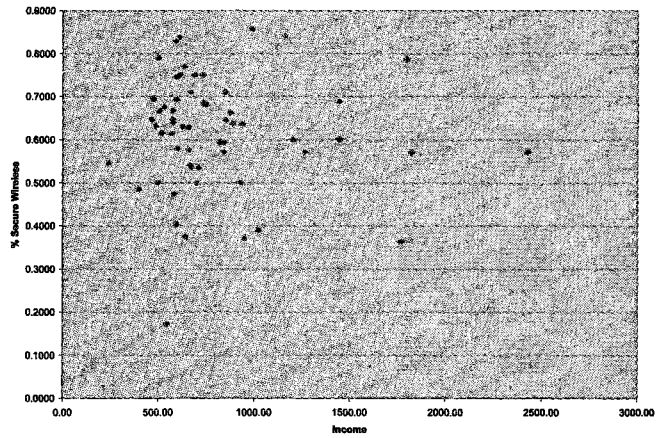


Chart 2: % Secure Wireless vs. Income



V. DISCUSSION AND FUTURE RESEARCH

In this study, none of the data tested under each hypothesis were found to be significant.[38] We cannot say with any certainty that income, population density, or education level have any effect on the expected level of wireless security.

These findings indicate that investing resources in large-scale educational campaigns to raise awareness of wireless security may be a misallocation of resources in the case of encryption for home-based wireless routers. Education levels had no statistically significant effect. The results also suggest that increasing levels of wireless security should not be expected to correlate with increasing wealth. In addition, users cannot be expected to protect themselves more effectively against increased risk to the extent that population density or a larger asset base indicates risk of misuse. There is no reason to assume that proposals to increase risk in the form of liability would be more effective than increased risk from housing density. Housing density is a visible and constant increase in the probability element of risk.[39] Liability would be invisible and not uniformly allocated. Thus arguments that are based on an informed, self-optimizing, technically competent self-securing public are flawed and proposals that are directed at altering the behavior of naïve users by allocating liability to those consumers are at best ineffective and potentially counterproductive.

One interesting result is an abnormally high percentage of access points with a default SSID but with encryption enabled from vendor 2Wire, available at http://www.2wire.com. Upon further research, it was found that 2Wire's wireless product comes with an installation wizard that walks a user through the setup which securely configures their access point. There were 340 2Wire routers with default SSIDs, or 13.9% of the total access points polled and 330 of those routers were secure, providing a 97% lockdown rate. Another set of fifty-seven routers identifiable as Linksys Secure Easy Setup models were found to have an 88% security rate. According to the Linksys website, available at http://linksys.com, these SES routers can be automatically configured to use encryption by pressing first a hardware button on the router and then a software button on a connected computer, eliminating the need for any decision making or manual configuration by the user. Removing these two types of routers from the data, we

[38] Each hypothesis was supported by the economics of information security.

[39] Risk = probability of an attack × potential loss.

found that only 55% of the other routers were configured by users to be secure. These figures are summarized in Table 3 below and they correspond closely with findings from a recent study that found that default settings on wireless routers are powerful indicators of security.[40]

Table 3: Wireless security levels by vendor

Router	*n*	*Secure*	*% Secure*
2Wire	340	330	0.971
Linksys SES	57	50	0.877
All others	2046	1116	0.545
Total	2443	1496	0.612

Defaults have been found to be extremely important in predicting behavior in several realms. Organ donation participation rates in countries where an opt-in mechanism was used were significantly higher than in countries where opt-out mechanisms were employed.[41] In the realm of software, Bellman, Johnson and Lohse found that default framings of opt-in/opt-out choices on a questionnaire had a significant effect on participation rates.[42] More specific to the question at hand, Sandvig and Shah found that default settings dominated user behavior with regard to wireless access point configuration.[43] It appears from the wardriving data that default settings do make a difference in the lockdown rate of home-based wireless routers.

An obvious response to this observation is a call for better interfaces that are specifically designed to provide scaffolding for uninformed consumers as they attempt to make decisions about wireless security and privacy risks. One possible scaffolding option

---

[40] Rajiv Shah and Christian Sandvig, "Software Defaults as De Facto Regulation: The Case of Wireless APs," *Information, Communication and Society* (forthcoming) http://web.si.umich.edu/tprc/papers/2005/427/TPRC%20Wireless%20Defaults.pdf (accessed October 31, 2007).

[41] Eric Johnson and Daniel Goldstein, "Do Defaults Save Lives?," *Science* 302, no. 5649 (2003): 1338–39.

[42] Steven Bellman, Eric J. Johnson, and Gerald L Lohse, "To Opt-In or Opt-Out? It Depends on the Question," *Communications of the ACM* 44, no. 2 (2001): 25–27.

[43] Shah and Sandvig, "Software Defaults as De Facto Regulation," 10–12.

might be a configuration wizard that walks a user through the process of locking down their router, just as the 2Wire routers provide. This could be considered a "usable security" approach that allows for assisted decision-making and potentially more flexible security outcomes.

Another option is that of the Linksys SES method, which removes all configuration responsibilities from the user other than the push of two buttons. This would be a "security as default" method, where all routers are configured to the same general security profile and consumer choices are severely limited.

The usable security paradigm would enable meaningful consumer choice and flexibility, for example, by allowing Internet sharing in lower income neighborhoods in a secure manner. The initial data indicates that this approach is slightly more effective than the security as default method, but further studies should focus on the relative merits of each approach.

One of the limitations of this study is that many of the locations in the study were college student locations and age was not taken into account in the study. Future research will include looking at age as a possible factor, with age cohorts representing years of computer use. However, obtaining this information is currently an unsolved research problem.

This has been an empirical study of *homo economus*, i.e. the self-optimizing risk-aware human of rational choice economic theory.[44] Other ongoing research involves behavioral studies such as an examination of the mental models of users with regard to wireless security as well as user awareness of privacy and security risks. Further studies will also focus on the usability differences between the two styles of secure router configuration. Formal usability analysis of wireless router installation and configuration is currently being undertaken by researchers in the Human-Computer Interaction program at the Indiana University School of Informatics. Use of those findings will allow us to better investigate our emergent hypothesis that only usability and default configuration predicts use of security in home-based wireless devices.

---

[44] A good overview of rational choice economic theory by John Scott of Essex University can be found at http://privatewww.essex.ac.uk/~scottj/socscot7.htm.

VI. CONCLUSION

The most effective predictors for secure wireless configuration are not rational choice factors such as income, education level or population density as might be inferred by early research in the economics of security. The best predictor is the type of router purchased by the consumer. Default settings and effective usability seem to be the driving forces behind wireless security. Thus, any policy aimed at increasing the security of the infrastructure by changing user behaviors should be grounded in enabling security through defaults and usability. Regardless of the policy investment in the rational model, end users will not implement the calculus of risk but will plug and play.

The most powerful determinants of wireless security in the home are the choices made in the factory. Neither increased risk nor increased levels of formal higher education alters consumer choices. Therefore, default configurations and usability are powerful determinants of the risk to consumers and security policies taking this into consideration should be adopted.